Japanese Patent Application Laid-open No. Hei 10-23548

Laid-open Date: January 23, 1998

[0046] Next, a schematic configuration of a communication system in which the portable storage device 1 and other plural electronic equipments transmit and receive signals wirelessly therebetween is shown in Fig. 2.

[0047] The portable storage device 1 performs wireless transmissions/receptions of encrypted signals to/from various electronic equipments, such as a facsimile machine 301, a so-called tower-type computer device 302, a high-performance and large-scale computer device 303, a so-called handheld computer device 304, a projector device 305, and a notebook-type personal computer device (hereinafter referred to as a PC) 306.

[0048] The electronic equipments having received the encrypted signals transmitted from the portable storage device 1 decrypt the encrypted signals to restore original data, and print or process the data.

[0049] As a method of encrypting/decrypting the data, "KEY PREDISTRIBUTION SYSTEM (hereinafter referred to as KPS): A method of sharing cryptographic key without communication," which is published in IEICE TRANSACTIONS of The Institute of Electronics, Information and Communication Engineers; A Vol. J71-A No. 11, pp. 2046-2053, November 1988, is used. In the method of

encrypting/decrypting the data by use of this KPS, the cryptographic key for use in encrypting and decrypting the data is previously shared among the electronic equipments which transmit/receive the data. The electronic equipments transmitting the data encrypt the data by use of the cryptographic key, and the electronic equipments receiving the data decrypt the received encrypted signals by use of the cryptographic key.

[0050] In order to create the cryptographic key for use in this KPS, each of the portable storage device 1, the facsimile machine 301, the tower-type computer device 302, the high-performance and large-scale computer device 303, the handheld computer device 304, the projector device 305, and the PC 306 includes unique identification information (hereinafter, referred to as a unique ID), and a unique and secret algorithm. Specifically, the portable storage device 1 stores the unique ID and the unique and secret algorithm in a memory provided in the encryption/decryption unit 20.

[0051] When a signal is to be transmitted/received between two electronic equipments in the communication system, first, the unique IDs are mutually transmitted/received, and the unique ID of the electronic equipment to which the signal should be transmitted is stored. Next, one of the electronic equipments which transmits the signal creates a cryptographic key by use of the received unique ID of the other electronic equipment and a secret

algorithm unique to itself, and encrypts the data by means of a cryptographic key program using this cryptographic key. Then, the one electronic equipment transmits an encrypted signal based on this encrypted data to the other electronic equipment. Moreover, the other electronic equipment also creates a cryptographic key by use of the received ID unique to the one electronic equipment and a secret program unique to itself, and decrypts the received encrypted signal according to a cryptographic key program using this cryptographic key to restore the original data.

[Fig. 2] A diagram for explaining transmissions/receptions of signals between the portable storage device and other electronic equipments.

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-023548
(43)Date of publication of application : 23.01.1998

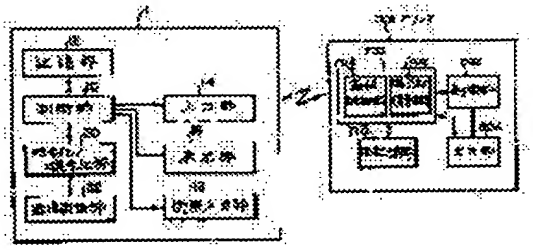
(51)Int.Cl. H04Q 7/38
G06F 9/06
G06K 17/00
G09C 1/00
H04L 9/08
// G06F 12/14

(21)Application number : 08-195709
(22)Date of filing : 05.07.1996

(71)Applicant : SEIKO EPSON CORP
(72)Inventor : MATSUI TETSUYA

(54) PORTABLE COMMUNICATION DEVICE AND PORTABLE STORAGE DEVICE

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a portable communication device and portable storage device which are portable electronic equipment equipped with various functions and can send and receive high-safety signals to and from other electronic equipment.
SOLUTION: Data read out of a storage part 12 are sent to a ciphering/ deciphering part 20 under the control of a control part 10. The ciphering/ deciphering part 20 generates a cipher key by using the ID characteristic of the other electronic equipment to which signals should be sent and the secret program characteristic of this equipment and ciphers the said data by a cipher key program using this cipher key. The ciphered data are sent to the said opposite electronic equipment through a communication control part 22.



LEGAL STATUS

[Date of request for examination] 03.07.2003
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's

decision of rejection]
[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平10－23548

(43)公開日　平成10年(1998)１月23日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｈ０４Ｑ	7/38			Ｈ０４Ｂ	7/26	１０９Ｓ
Ｇ０６Ｆ	9/06	５５０		Ｇ０６Ｆ	9/06	５５０Ｚ
Ｇ０６Ｋ	17/00			Ｇ０６Ｋ	17/00	Ｅ
Ｇ０９Ｃ	1/00	６３０	7259－５Ｊ	Ｇ０９Ｃ	1/00	６３０Ｄ
Ｈ０４Ｌ	9/08			Ｇ０６Ｆ	12/14	３２０Ｂ

審査請求　未請求　請求項の数13　ＦＤ　（全 12 頁）　最終頁に続く

(21)出願番号　特願平8－195709

(22)出願日　平成８年(1996)７月５日

(71)出願人　000002369
セイコーエプソン株式会社
東京都新宿区西新宿２丁目４番１号

(72)発明者　松井　哲也
長野県諏訪市大和３丁目３番５号　セイコーエプソン株式会社内

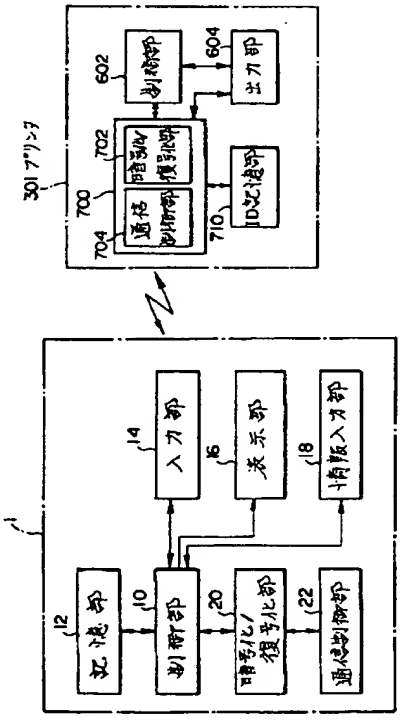
(74)代理人　弁理士　井上　一　（外２名）

(54)【発明の名称】　携帯型通信装置及び携帯型記憶装置

(57)【要約】

【課題】　様々な機能を備える携帯型の電子機器であって、他の電子機器との間で、安全性の高い信号の送受信を行うことができる携帯型通信装置及び携帯型記憶装置を提供すること。

【解決手段】　制御部１０の制御により記憶部１２から読み出されたデータは、暗号化／復号化部２０に送られる。暗号化／復号化部２０は、信号を送信すべき他の電子機器の固有のＩＤ及び自機の固有の秘密プログラムを用いて暗号鍵を生成し、この暗号鍵を用いた暗号鍵プログラムにより前記データを暗号化する。この暗号化されたデータは、通信制御部２２を介して前記他の電子機器に送信される。



1

【特許請求の範囲】

【請求項１】　携帯して信号を送受信する携帯型通信装置において、

他の電子機器との間で、情報を送受信する通信手段と、

前記他の電子機器の固有の識別情報及び自機の固有の秘密アルゴリズムを用いてデータを変換し、前記通信手段を介して前記変換したデータによる変換信号を前記他の電子機器に送信する変換手段と、

前記変換信号の送受信動作に先立って、前記通信手段を介して、自機の固有の識別情報を前記他の電子機器に送信し、前記他の電子機器の固有の識別情報を受信する制御手段と、を備えることを特徴とする携帯型通信装置。

【請求項２】　請求項１において、

前記変換信号は、暗号化信号であることを特徴とする携帯型通信装置。

【請求項３】　請求項２において、

前記変換手段は、前記他の電子機器の固有の識別情報及び自機の固有の秘密アルゴリズムを用いて暗号鍵を生成し、この暗号鍵を用いた暗号鍵プログラムにより前記データを暗号化する暗号化手段であることを特徴とする携帯型通信装置。

【請求項４】　請求項２、３のいずれかにおいて、

前記変換手段は、前記他の電子機器から送信された暗号化信号を、前記他の電子機器の固有の識別情報及び自機の固有の秘密アルゴリズムを用いて復号化する復号化手段を含むことを特徴とする携帯型通信装置。

【請求項５】　請求項４において、

前記復号化手段は、前記他の電子機器の固有の識別情報及び自機の固有の秘密アルゴリズムを用いて暗号鍵を生成し、この暗号鍵を用いた暗号鍵プログラムにより信号を復号化することを特徴とする携帯型通信装置。

【請求項６】　請求項２～５のいずれかにおいて、

携帯型通信装置本体に着脱自在に装着され、固有の識別情報、固有の秘密アルゴリズム、及びデータを記憶する携帯型記憶媒体と、

前記携帯型記憶媒体から前記固有の識別情報、前記固有の秘密アルゴリズム、及び前記データを読み出す情報入力手段と、を含み、

前記制御手段は、前記通信手段を介して、前記情報入力手段からの前記固有の識別情報を前記他の電子機器に送信し、前記他の電子機器の固有の識別情報を受信し、

前記暗号化手段は、前記他の電子機器の固有の識別情報及び前記自機の固有の秘密アルゴリズムを用いて暗号鍵を生成し、この暗号鍵を用いた暗号鍵プログラムにより前記データを暗号化して暗号化信号を生成し、

前記通信手段は、前記暗号化信号を前記他の電子機器に送信することを特徴とする携帯型通信装置。

【請求項７】　情報を記憶する携帯型記憶装置において、データを記憶する記憶手段と、

他の電子機器との間で、情報を送受信する通信手段と、

2

前記他の電子機器の固有の識別情報及び自機の固有の秘密アルゴリズムを用いて、前記記憶手段に記憶されるデータを変換し、前記通信手段を介して前記変換したデータによる変換信号を前記他の電子機器に送信する変換手段と、

前記変換信号の送受信動作に先立って、前記通信手段を介して、自機の固有の識別情報を前記他の電子機器に送信し、前記他の電子機器の固有の識別情報を受信する制御手段と、を備えることを特徴とする携帯型記憶装置。

【請求項８】　請求項７において、

前記変換信号は、暗号化信号であることを特徴とする携帯型記憶装置。

【請求項９】　請求項８において、

前記変換手段は、前記他の電子機器の固有の識別情報及び自機の固有の秘密アルゴリズムを用いて暗号鍵を生成し、この暗号鍵を用いた暗号鍵プログラムにより前記データを暗号化する暗号化手段であることを特徴とする携帯型記憶装置。

【請求項１０】　請求項８、９のいずれかにおいて、

前記変換手段は、前記他の電子機器から送信された暗号化信号を、前記他の電子機器の固有の識別情報及び自機の固有の秘密アルゴリズムを用いて復号化する復号化手段を含むことを特徴とする携帯型記憶装置。

【請求項１１】　請求項１０において、

前記復号化手段は、前記他の電子機器の固有の識別情報及び自機の固有の秘密アルゴリズムを用いて暗号鍵を生成し、この暗号鍵を用いた暗号鍵プログラムにより信号を復号化することを特徴とする携帯型記憶装置。

【請求項１２】　請求項１０、１１のいずれかにおいて、

前記制御手段は、前記暗号化手段で前記記憶手段に記憶するデータを暗号化して暗号化信号を生成し、この暗号化信号を前記通信手段を介して前記他の電子機器に送信した後、前記他の電子機器で処理されたデータを暗号化した暗号化信号を前記通信手段で受信して、前記復号化手段で復号化することを特徴とする携帯型記憶装置。

【請求項１３】　請求項１０～１２のいずれかに記載する携帯型記憶装置を備えて成ることを特徴とする携帯型電話装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、携帯して信号を送受信する携帯型通信装置及び情報を記憶する携帯型記憶装置に関する。

【０００２】

【背景技術】従来、屋内で、パーソナルコンピュータ装置（以下、ＰＣという）を常時使用している人は、屋外でも使用したいという要望があった。この要望に応じて、ＰＣやプリンタ装置等の電子機器を備え、ユーザーに対して、前記電子機器の使用の提供を専門とする仕事

が開始されている。

【０００３】また、将来、例えばコンビニエンスストアや喫茶店等で、ＰＣやプリンタ装置等の電子機器を備え、来店するお客に対して、前記電子機器の使用を提供することが考えられる。

【０００４】このとき、ユーザーは、フロッピィディスクやメモリカード等の携帯型記憶媒体を前記コンビニエンスストアや喫茶店に持参して、前記設置されたＰＣやプリンタ装置に前記携帯型記憶媒体を装着し、前記携帯型記憶媒体に記憶されているデータを処理したり、前記データを他のＰＣ等の電子機器に送信したりすることが可能となる。このように、ユーザーは、前記携帯型記憶媒体のみを持参して、他の電子機器との間で情報の送受信を行うことが可能となる。

【０００５】

【発明が解決しようとする課題】ところが、上述したシステムでは、前記携帯型記憶媒体を、ＰＣやプリンタ装置等の電子機器に直接に装着して、その携帯型記憶媒体に記憶されるデータを読み出す。従って、例えば、前記電子機器内にいわゆるコンピュータ・ウィルスが存在する場合には、このコンピュータ・ウィルスが前記携帯型記憶媒体に侵入して、前記携帯型記憶媒体内に記憶されるデータを壊したり、また、前記コンピュータ・ウィルスが侵入した携帯型記憶媒体を他の電子機器で使用した場合には、この電子機器内のデータを破壊したりするおそれが生じる。

【０００６】さらに、前記携帯型記憶媒体に記憶されるデータを、前記電子機器に内蔵されるハードディスク等の記憶手段に記憶させて処理したときに、その処理したデータを、前記電子機器の記憶手段内に残したままにしてしまうときがある。このとき、前記処理したデータが秘密データである場合には、その処理したデータを他人に盗まれて、その安全性を保てないおそれが生じる。

【０００７】本発明は、このような課題を鑑みてなされたものであり、その目的は、様々な機能を備える携帯型の電子機器であって、他の電子機器との間で、安全性の高い信号の送受信を行うことができる携帯型通信装置及び携帯型記憶装置を提供することにある。

【０００８】

【課題を解決するための手段】上記課題を解決するために、請求項１の発明は、携帯して信号を送受信する携帯型通信装置において、他の電子機器との間で、情報を送受信する通信手段と、前記他の電子機器の固有の識別情報及び自機の固有の秘密アルゴリズムを用いてデータを変換し、前記通信手段を介して前記変換したデータによる変換信号を前記他の電子機器に送信する変換手段と、前記変換信号の送受信動作に先立って、前記通信手段を介して、自機の固有の識別情報を前記他の電子機器に送信し、前記他の電子機器の固有の識別情報を受信する制御手段と、を備えることを特徴とする。

【０００９】本発明に係る携帯型通信装置は、任意の場所から、他の電子機器に対して、変換したデータを送信する。この携帯型通信装置は、屋内で、所望の他の電子機器にデータを送信する場合の他に、屋外の所望の他の電子機器が存在する場所近傍まで持ち出されて、前記他の電子機器にデータを送信する場合がある。ここで、屋外において送信されるデータは、屋内において送信されるデータよりも、第三者に盗まれるおそれが多くなる。

【００１０】このように、屋内及び屋外で送信されるデータを盗まれた場合にも、このデータを解読することは困難であり、より安全性の高いデータを送信することができる。

【００１１】請求項２の発明は、請求項１において、前記変換信号は、暗号化信号であることを特徴とする。

【００１２】ここで、前記携帯型通信装置及び前記他の電子機器がそれぞれ備える、固有の識別情報及び固有の秘密アルゴリズムは、例えば、電子情報通信学会論文誌ＡVol.J71-A No.11 pp.2046-2053 1988年11月で提案されている、固有の識別情報及び固有の秘密アルゴリズムを用いて暗号鍵を生成し、この暗号鍵を用いた暗号鍵プログラムによりデータを暗号化する方法である、暗号鍵を通信なしで共有する方法：KEY PREDISTRIBUTION SYSTEM（以下、ＫＰＳという）で用いられる、前記固有の識別情報及び前記固有の秘密アルゴリズムである。この暗号鍵を生成するには、携帯型通信装置では、前記他の電子機器の固有の識別情報と自機の固有の秘密アルゴリズムを用い、前記他の電子機器では、前記携帯型通信装置の固有の識別情報及び自機の固有の秘密アルゴリズムを用いる。

【００１３】このＫＰＳによって、携帯型通信装置で暗号化されたデータは、前記他の電子機器の固有の識別情報及び自機の固有の秘密アルゴリズムを用いなければ復号化することは困難であり、前記他の電子機器で暗号化されたデータは、前記携帯型通信装置の固有の識別情報及び自機の固有の秘密アルゴリズムを用いなければ復号化することは困難であるので、送信されるデータの安全性を高めることができる。

【００１４】請求項３の発明は、請求項２において、前記変換手段は、前記他の電子機器の固有の識別情報及び自機の固有の秘密アルゴリズムを用いて暗号鍵を生成し、この暗号鍵を用いた暗号鍵プログラムにより前記データを暗号化する暗号化手段であることを特徴とする。

【００１５】これにより、データを送信するときに、前記固有の識別情報及び前記固有の秘密アルゴリズムを用いて、前記ＫＰＳによるデータの暗号化を行うことができる。

【００１６】このＫＰＳにより暗号化されたデータは、その送信時に盗まれた場合にも、前記暗号鍵を使用しなければ、復号化することは困難であるので、送信時のデータの安全性を高めることができる。

5

【００１７】請求項４の発明は、請求項２、３のいずれかにおいて、前記変換手段は、前記他の電子機器から送信された暗号化信号を、前記他の電子機器の固有の識別情報及び自機の固有の秘密アルゴリズムを用いて復号化する復号化手段を含むことを特徴とする。

【００１８】これにより、他の電子機器から送信される、ＫＰＳを用いて暗号化されたデータの暗号化信号を、復号化して、元のデータを復元することができる。

【００１９】請求項５の発明は、請求項４において、前記復号化手段は、前記他の電子機器の固有の識別情報及び自機の固有の秘密アルゴリズムを用いて暗号鍵を生成し、この暗号鍵を用いた暗号鍵プログラムにより信号を復号化することを特徴とする。

【００２０】前記ＫＰＳに用いた復号化を行う際に用いる暗号鍵を、前記送信された他の電子機器の固有の識別情報及び自機の固有の秘密アルゴリズムを用いて生成するので、前記暗号鍵を簡易に生成することができる。

【００２１】請求項６の発明は、請求項２～５のいずれかにおいて、携帯型通信装置本体に着脱自在に装着され、固有の識別情報、固有の秘密アルゴリズム、及びデータを記憶する携帯型記憶媒体と、前記携帯型記憶媒体から前記固有の識別情報、前記固有の秘密アルゴリズム、及び前記データを読み出す情報入力手段と、を含み、前記制御手段は、前記通信手段を介して、前記情報入力手段からの前記固有の識別情報を前記他の電子機器に送信し、前記他の電子機器の固有の識別情報を受信し、前記暗号化手段は、前記他の電子機器の固有の識別情報及び前記自機の固有の秘密アルゴリズムを用いて暗号鍵を生成し、この暗号鍵を用いた暗号鍵プログラムにより前記データを暗号化して暗号化信号を生成し、前記通信手段は、前記暗号化信号を前記他の電子機器に送信することを特徴とする。

【００２２】この携帯型記憶装置を用いることにより、前記携帯型記憶媒体を前記他の電子機器に装着することなく、前記携帯型記憶媒体に記憶されるデータを前記他の電子機器に送信して、処理することができる。よって、前記携帯型記憶媒体に、前記他の電子機器内のデータが侵入することを防止できる。

【００２３】具体的には、例えば、前記他の電子機器内に、いわゆるコンピュータ・ウィルスが存在する場合には、このコンピュータ・ウィルスが前記携帯型記憶媒体に侵入して、この携帯型記憶媒体内のデータを破壊したり、さらには、前記携帯型記憶媒体を装着した電子機器に前記携帯型記憶媒体内のコンピュータ・ウィルスが侵入して、前記電子機器内のデータを破壊したりすることを防止できる。

【００２４】請求項７の発明は、情報を記憶する携帯型記憶装置において、データを記憶する記憶手段と、他の電子機器との間で、情報を送受信する通信手段と、前記他の電子機器の固有の識別情報及び自機の固有の秘密アルゴリズムを用いて、前記記憶手段に記憶されるデータを変換し、前記通信手段を介して前記変換したデータによる変換信号を前記他の電子機器に送信する変換手段と、前記変換信号の送受信動作に先立って、前記通信手段を介して、自機の固有の識別情報を前記他の電子機器に送信し、前記他の電子機器の固有の識別情報を受信する制御手段と、を備えることを特徴とする。

6

【００２５】このように、ユーザは、任意の場所から他の電子機器に対して、内部に記憶するデータを変換して送信する。これにより、このデータの送信時にデータが盗まれた場合にも、データを解読することは困難となるので、より安全性の高い信号として送信することができる。

【００２６】請求項８の発明は、請求項７において、前記変換信号は、暗号化信号であることを特徴とする。

【００２７】データは、前記ＫＰＳによって、前記他の電子機器の固有の識別情報及び自機の固有の秘密アルゴリズムを用いて暗号化されており、この暗号化されたデータは、前記携帯型通信装置の固有の識別情報及び前記他の電子機器の固有の秘密アルゴリズムを用いなければ、復号化することは困難であるので、送信時のデータの安全性を高めることができる。

【００２８】請求項９の発明は、請求項８において、前記変換手段は、前記他の電子機器の固有の識別情報及び自機の固有の秘密アルゴリズムを用いて暗号鍵を生成し、この暗号鍵を用いた暗号鍵プログラムにより前記データを暗号化する暗号化手段であることを特徴とする。

【００２９】これにより、データを送信するときに、前記固有の識別情報及び前記固有の秘密アルゴリズムを用いて、前記ＫＰＳによるデータの暗号化を行うことができる。

【００３０】このＫＰＳにより暗号化されたデータは、その送信時に盗まれた場合にも、前記暗号鍵を使用しなければ、復号化することは困難であるので、送信時のデータの安全性を高めることができる。

【００３１】請求項１０の発明は、請求項８、９のいずれかにおいて、前記変換手段は、前記他の電子機器から送信された暗号化信号を、前記他の電子機器の固有の識別情報及び自機の固有の秘密アルゴリズムを用いて復号化する復号化手段を含むことを特徴とする。

【００３２】これにより、前記ＫＰＳを用いて暗号化されたデータの暗号化信号を、復号化して、元のデータを復元することができる。

【００３３】請求項１１の発明は、請求項１０において、前記復号化手段は、前記他の電子機器の固有の識別情報及び自機の固有の秘密アルゴリズムを用いて暗号鍵を生成し、この暗号鍵を用いた暗号鍵プログラムにより信号を復号化することを特徴とする。

【００３４】前記ＫＰＳに用いた復号化を行う際に用いる暗号鍵を、前記送信された他の電子機器の固有の識別

情報及び自機の固有の秘密アルゴリズムを用いて生成するので、前記暗号鍵を簡易に生成することができる。

【００３５】請求項１２の発明は、請求項１０、１１のいずれかにおいて、前記制御手段は、前記暗号化手段で前記記憶手段に記憶するデータを暗号化して暗号化信号を生成し、この暗号化信号を前記通信手段を介して前記他の電子機器に送信した後、前記他の電子機器で処理されたデータを暗号化した暗号化信号を前記通信手段で受信して、前記復号化手段で復号化することを特徴とする。

【００３６】これにより、記憶するデータを処理速度の速い他の電子機器で迅速に処理することができる。このとき、前記データを暗号化信号に変換して送信するので、前記データの送信時に、前記データを盗まれた場合にも、前記データを解読することが困難となり、データの安全性を高めることができる。

【００３７】請求項１３の発明は、請求項１０～１２のいずれかに記載する携帯型記憶装置を備えて成る携帯型電話装置であることを特徴とする。

【００３８】このように、１つの電子機器が、携帯型記憶装置の機能及び携帯型電話装置の機能を備えるので、ユーザは、２つの電子機器をそれぞれ携帯する必要がなくなり、多機能の電子機器を簡易に携帯することができる。

【００３９】

【発明の実施の形態】次に、本発明の好適な実施の形態を説明する。

【００４０】図１は、本発明に係る携帯型通信装置を含む携帯型記憶装置の概略的な構成を示す。

【００４１】まず、携帯型記憶装置１の第１の実施の形態について、以下に説明する。

【００４２】この図１の携帯型記憶装置１は、人が携帯して利用可能な大きさであり、他の電子機器と情報を送受信する通信手段である通信制御部２２と、前記他の電子機器の固有の識別情報及び自機の固有の秘密アルゴリズムを用いてデータを変換し、前記通信手段を介して前記変換したデータによる変換信号を前記他の電子機器に送信する変換手段である暗号化／復号化部２０と、前記変換信号の送受信動作に先立って、前記通信手段を介して、自機の固有の識別情報を前記他の電子機器に送信し、前記他の電子機器の固有の識別情報を受信する制御手段である制御部１０とを備える。

【００４３】また、この携帯型記憶装置１は、ユーザの操作により、命令や情報を入力する入力部１４と、制御部１０で制御されるデータ等を表示する表示部１６とを備える。前記入力部１４は、キーボードやペン等の入力操作を行うことができるものである。前記表示部１６は、液晶パネル等を用いたディスプレイ装置である。また、タッチパネルを用いることにより、前記入力部１４を前記表示部１６上に設けることも可能である。

【００４４】さらに、この携帯型記憶装置１は、データを記憶する、大容量の記憶手段である記憶部１２を備える。これにより、携帯型記憶装置１の内部の記憶部１２に記憶されるデータを他の電子機器に送信することができる。

【００４５】この記憶部１２のデータを他の電子機器に送信するときには、制御部１０の制御により、記憶部１２のデータが読み出されて、暗号化／復号化部２０に送られる。このデータは、暗号化／復号化部２０で暗号化される。この暗号化されたデータは、通信制御部２２の制御により、暗号化信号として、他の電子機器に送信される。また、他の電子機器から送信される暗号化信号は、通信制御部２２で受信されて、暗号化／復号化部２０に送られる。この暗号化／復号化部２０では、暗号化信号を復号化する。これにより、復号化されたデータは、制御部１０の制御により、記憶部１２に記憶される。

【００４６】次に、携帯型記憶装置１と他の複数の電子機器とがワイヤレスで信号を送受信する通信システムの概略的な構成を、図２に示す。

【００４７】この携帯型記憶装置１は、例えば、ファクシミリ装置３０１や、いわゆるタワー型のコンピュータ装置３０２や、高性能な大型コンピュータ装置３０３や、いわゆるハンドヘルド・コンピュータ装置３０４や、プロジェクタ装置３０５や、ノートブック型のパーソナルコンピュータ装置（以下、ＰＣという）３０６等の様々な電子機器と、ワイヤレスに暗号化信号の送受信を行う。

【００４８】携帯型記憶装置１から送信される暗号化信号を受信した電子機器は、前記暗号化信号を復号化して元のデータを復元し、このデータを印刷したり、処理したりする。

【００４９】このデータの暗号化／復号化方法としては、電子情報通信学会論文誌　Ａ　Vol.J71-A No.11 pp.2046-2053 1988年11月に掲載される、暗号鍵を通信なしで共有する方法：KEY PREDISTRIBUTION SYSTEM（以下、ＫＰＳという）を用いる。このＫＰＳを用いたデータの暗号化／復号化方法では、データを暗号化及び復号化するときに用いる暗号鍵を、データを送受信する電子機器間で予め共有しておき、データを送信する電子機器では、前記暗号鍵を用いてデータを暗号化し、データを受信する電子機器では、受信した暗号化信号を前記暗号鍵を用いて復号化する。

【００５０】このＫＰＳで用いる暗号鍵を生成するために、携帯型記憶装置１、ファクシミリ装置３０１、タワー型のコンピュータ装置３０２、高性能な大型コンピュータ装置３０３、ハンドヘルド・コンピュータ装置３０４、プロジェクタ装置３０５、及びＰＣ３０６は、固有の識別情報（以下、固有のＩＤという）及び固有の秘密アルゴリズムをそれぞれ備える。具体的には、携帯型記

憶装置１は、暗号化／復号化部２０内に備えるメモリ等に、固有のＩＤ及び固有の秘密アルゴリズムを記憶する。

【００５１】前記通信システム内の２つの電子機器で、信号を送受信するときには、まず、固有のＩＤを相互に送受信して、信号を送信すべき電子機器の固有のＩＤを記憶する。次に、信号を送信する一方の電子機器は、前記受信した他方の電子機器の固有のＩＤ及び自機の固有の秘密アルゴリズムを用いて暗号鍵を生成し、この暗号鍵を用いた暗号鍵プログラムによりデータを暗号化する。そして、この暗号化したデータによる暗号化信号を、他方の電子機器に送信する。また、他方の電子機器も、前記受信した一方の電子機器の固有のＩＤ及び固有の秘密プログラムを用いて暗号鍵を生成し、この暗号鍵を用いた暗号鍵プログラムにより、受信した暗号化信号を復号化して元のデータを復元する。

【００５２】次に、前記通信システムのうちの、携帯型記憶装置１とプリンタ装置３０１との通信について説明する。

【００５３】プリンタ装置３０１は、データを印刷する出力部６０４と、他の電子機器との間で信号を送受信する通信部７００と、ＩＤ記憶部７１０と、前記各部の動作を制御する制御部６０２とを備える。

【００５４】通信部７００は、暗号化／復号化部７０２及び通信制御部７０４を備える。この前記暗号化／復号化部７０２は、携帯型記憶装置１の暗号化／復号化部２０と同様の機能を備え、通信制御部７０４は携帯型記憶装置１の通信制御部２２と同様の機能を備える。ＩＤ記憶部７１０は、このプリンタ装置３０１の固有のＩＤ及び固有の秘密アルゴリズムが記憶されたＩＣである。

【００５５】まず、携帯型記憶装置１の固有のＩＤ及びプリンタ装置３０１の固有のＩＤの送受信について説明する。

【００５６】携帯型記憶装置１は、制御部１０の制御により、プリンタ装置３０１に対して、プリンタ装置３０１の固有のＩＤの送信要求命令を送信する。

【００５７】プリンタ装置３０１は、前記固有のＩＤの送信要求命令を通信制御部７０４で受信する。この受信した固有のＩＤの送信要求命令は、制御部６０２に送られる。制御部６０２は、前記受信した固有のＩＤの送信要求命令に応じて、通信部７００を制御する。通信部７００は、ＩＤ記憶部７１０から固有のＩＤを読み出す。このプリンタ装置３０１の固有のＩＤは、通信制御部７０４の制御により、携帯型記憶装置１に送信される。

【００５８】携帯型記憶装置１は、前記送信されたプリンタ装置３０１の固有のＩＤを、通信制御部２２で受信し、暗号化／復号化部２０に記憶する。また、暗号化／復号化部２０は、この携帯型記憶装置１の固有のＩＤを読み出す。この固有のＩＤは、通信制御部５０４の制御により、プリンタ装置３０１に送信される。

【００５９】プリンタ装置３０１は、前記送信された携帯型記憶装置１の固有のＩＤを、通信制御部７０４で受信して、記憶する。

【００６０】次に、データの暗号化及び復号化について説明する。

【００６１】固有のＩＤの送受信後、携帯型記憶装置１の暗号化／復号化部２０では、プリンタ装置３０１の固有のＩＤ及び自機の固有の秘密プログラムを用いて暗号鍵を生成する。

【００６２】例えば、携帯型記憶装置１の記憶部１２に記憶されているデータを送信するときには、制御部１０からの制御により、前記記憶部１２に記憶されるデータが、暗号化／復号化部２０に送られる。暗号化／復号化部２０では、前記生成した暗号鍵を用いた暗号鍵プログラムにより、前記送られたデータを暗号化する。この暗号化された暗号化信号は、通信制御部２２の制御により、プリンタ装置３０１に送信される。

【００６３】携帯型記憶装置１から送信された暗号化信号は、プリンタ装置３０１の通信制御部７０４で受信されて、暗号化／復号化部７０２に送られる。この暗号化／復号化部７０２では、前記受信した携帯型記憶装置１の固有のＩＤ及び自機の固有の秘密プログラムを用いて暗号鍵を生成する。そして、この暗号鍵を用いた暗号鍵プログラムにより、前記受信した暗号化信号を復号化する。これにより、暗号化される前のデータが復元される。この復元された元のデータは、制御部６０２の制御により、出力部６０４に送られる。そして、出力部６０４により、データが印刷されて出力される。

【００６４】このように、携帯型記憶装置１とプリンタ装置３０１との間では、記憶部１２に記憶されるデータを暗号化して送信し、受信した暗号化信号を復号化する。

【００６５】ここで、従来のデータの暗号化方式では、データを暗号化するときに用いる暗号鍵及び暗号化データを復号化するときに用いる復号鍵は、例えば、暗号鍵及び復号鍵を管理する管理システム等から通信によって配送されることにより得ている。これに対して、ＫＰＳを用いたデータの暗号化／復号化を行うことにより、携帯型記憶装置１及びプリンタ装置３０１は、暗号鍵及び復号鍵を内部で生成するので、前記暗号鍵及び復号鍵を簡易に得ることができる。また、前記管理システムを設置する必要がなく、前記管理システムの設備にかかる費用等を削減することができる。さらに、暗号化したデータが、その送信中に第三者に傍受されて盗まれた場合にも、その暗号化したデータを解読することは困難であるので、データの安全性を保つことができる。

【００６６】尚、固有のＩＤとして、携帯型記憶装置１のユーザの名前、電話番号、電子メールのアドレス等の、データを送受信する電子機器間で予め知っている情報を用いることにより、固有のＩＤを予め用意する必要

がなくなるので、データの暗号化／復号化をさらに簡易に行うことができる。

【００６７】次に、携帯型記憶装置１のデータをプリンタ装置３０１で印刷するときの、携帯型記憶装置１とプリンタ装置３０１との信号の送受信の手順について、図３のフローチャートを用いて説明する。

【００６８】まず、ステップＳ２で、携帯型記憶装置１では、記憶部１２に記憶するデータのファイル名を、入力部１４を操作して指定する。

【００６９】次に、ステップＳ４で、ユーザは、入力部１４を操作して、表示部１６に表示される印刷コマンド等を選択する。この入力命令は、制御部１０に送られる。

【００７０】このとき、ステップＳ２２で、プリンタ装置３０１は、電源がＯＮであってプリント可能な状態、いわゆるスタンバイ状態となっているものとする。

【００７１】次に、ステップＳ６で、携帯型記憶装置１の制御部１０は、プリンタ装置３０１に対して、ＩＤの送信要求命令を送信する。

【００７２】ステップＳ２４で、プリンタ装置３０１は、前記ＩＤの送信要求命令を受信し、このＩＤの送信要求命令に応じて、固有のＩＤを携帯型記憶装置１に送信する。

【００７３】携帯型記憶装置１は、プリンタ装置３０１から送信されるプリンタ装置３０１の固有のＩＤを受信して記憶する。また、携帯型記憶装置１は、自機の固有のＩＤをプリンタ装置３０１に送信する。

【００７４】プリンタ装置３０１は、携帯型記憶装置１の固有のＩＤを受信して記憶する。

【００７５】この後、ステップＳ１２で、携帯型記憶装置１は、プリンタ装置３０１の固有のＩＤ及び自機の固有の秘密プログラムを用いて暗号鍵を生成する。また、ステップＳ２６で、プリンタ装置３０１は、携帯型記憶装置１の固有のＩＤ及び自機の固有の秘密アルゴリズムを用いて暗号鍵を生成する。

【００７６】次に、ステップＳ１４で、携帯型記憶装置１は、生成した暗号鍵を用いた暗号鍵プログラムにより、印刷用のデータを暗号化する。そして、この暗号化した印刷用データ及びこの印刷用データを印刷するときの制御用データである印刷制御用コードをプリンタ装置３０１に送信する。

【００７７】一方、ステップＳ２８で、プリンタ装置３０１は、暗号化された印刷用データ及び印刷制御用コードを受信する。

【００７８】そして、ステップＳ３０で、暗号化された印刷用データを復号化して、元の印刷用データを復元する。この後、受信した印刷制御用コードに基づいて、印刷用データを印刷する。また、印刷が正常に行われたか否か等を示す印刷制御用コードを、携帯型記憶装置１に対して送信する。携帯型記憶装置１は、プリンタ装置３０１からの印刷制御用コードを受信し、この印刷制御用コードに基づいて、プリンタ装置３０１で印刷が正常に行われたか否かを判別する。

【００７９】次に、携帯型記憶装置１の第２の実施の形態について説明する。

【００８０】この携帯型記憶装置１は、着脱自在に装着され、固有の識別情報、固有の秘密アルゴリズム、及びデータを記憶する携帯型記憶媒体と、前記携帯型記憶媒体から前記固有の識別情報、前記固有の秘密アルゴリズム、及び前記データを読み出す情報入力手段である情報入力部１８とを含む。この携帯型記憶媒体としては、例えばＩＣカードを用いることができる。

【００８１】この携帯型記憶装置１が他の電子機器と信号を送受信するときにも、まず、固有のＩＤを他の電子機器と送受信した後に、信号を送信する側である携帯型記憶装置１ではデータを暗号化して送信し、信号を受信する側である他の電子機器では、送信された暗号化信号を復号化してデータを復元する。

【００８２】まず、制御部１０の制御により、情報入力部１８に装着される前記携帯型記憶媒体から、自機の電子機器の固有のＩＤ、自機の固有の秘密プログラム、及びデータが読み出される。前記自機の電子機器の固有のＩＤは、制御部１０の制御により、通信制御部２２を介して他の電子機器に送信される。また、他の電子機器の固有のＩＤを、通信制御部２２で受信して、記憶する。

【００８３】この後、携帯型記憶装置１は、前記自機の固有の秘密プログラム及びデータを、暗号化／符号化部２０に送る。この暗号化／符号化部２０は、前記他の電子機器の固有のＩＤ及び自機の固有の秘密プログラムを用いて暗号鍵を生成し、この暗号鍵を用いた暗号鍵プログラムにより前記データを暗号化する。この暗号化信号は、通信制御部２２を介して他の電子機器に送信される。

【００８４】また、暗号化信号を受信したときには、暗号化信号は、通信制御部２２を介して暗号化／復号化部２０に送られる。暗号化／復号化部２０は、前記暗号化信号を、前記暗号鍵を用いた暗号鍵プログラムにより復号化して、データを復元する。この復元されたデータは、制御部１０の制御により、前記携帯型記憶媒体に書き込まれる。

【００８５】例えば、図４に示すように、携帯型記憶装置１には、情報入力部１８であるＩＣカード挿入部が設けられ、このＩＣカード挿入部に携帯型記憶媒体であるＩＣカード１０１を挿入するものである。この携帯型記憶装置１は、コンピュータ装置１００と、前記ＩＣカード１０１に記憶されるデータを送受信する。

【００８６】具体的には、例えば、ＩＣカード１０１は、ネットワークを通じた電子商取引（エレクトロニック・コマース：electronic commerce）において、電子的な決済に用いるプリペイドカードや、キャッシュカー

ドや、クレジットカード等とすることが考えられる。このとき、前記コンピュータ装置１００は、例えば、複数のコンピュータ装置等が相互に接続されたネットワークであって、商業的な取引が行われる、いわゆるサイバーモールに接続される端末となる。

【００８７】携帯型記憶装置１のＩＣカード１０１には、ＩＣ１０２が組み込まれている。

【００８８】このＩＣ１０２に、自機の固有のＩＤ、自機の固有の秘密アルゴリズム及びデータが記憶される。携帯型記憶装置１の制御部１０は、前記自機の固有のＩＤを読み出して、通信制御部２２を介してコンピュータ装置１００に送信し、また、コンピュータ装置１００の固有のＩＤを受信する。

【００８９】携帯型記憶装置１の制御部１０は、前記自機の固有の秘密アルゴリズムをＩＣカード１０１のＩＣ１０２から読み出し、この自機の固有の秘密アルゴリズムを暗号化／復号化部２０に送る。暗号化／復号化部２０は、この自機の固有の秘密アルゴリズムと前記コンピュータ装置１００の固有のＩＤとを用いて暗号鍵を生成する。さらに、携帯型記憶装置１の制御部１０は、ＩＣ１０２からデータを読み出し、このデータを暗号化／復号化部２０に送る。暗号化／復号化部２０は、前記データを前記暗号鍵を用いた暗号鍵プログラムで暗号化する。この暗号化されたデータは、暗号化信号として通信制御部２２を介してコンピュータ装置１００に送信される。

【００９０】このコンピュータ装置１００は、暗号化信号を受信したときには、携帯型記憶装置１の固有のＩＤ及び自機の固有の秘密アルゴリズムを用いて暗号鍵を生成し、この暗号鍵を用いた暗号鍵プログラムで前記暗号化信号を復号化する。そして、コンピュータ装置１００は、復号化された元のデータを処理する。このとき、必要に応じて、前記データをサイバーモール内の他のコンピュータ装置に送信して処理する場合もある。この後、コンピュータ装置１００は、前記処理されたデータを暗号化し、この暗号化信号を携帯型記憶装置１に送信する。

【００９１】携帯型記憶装置１は、前記暗号化信号を通信制御部２２で受信し、暗号化／復号化部２０に送る。前記暗号化信号は、この暗号化／復号化部２０で前記暗号鍵を用いた暗号鍵プログラムにより復号化されて、データが復元される。この復元されたデータは、制御部１０の制御により、ＩＣカード１０１のＩＣ１０２に書き込まれる。

【００９２】例えば、ＩＣカード１０１をプリペイドカードとして用いるときには、ＩＣカード１０１のＩＣ１０２に記憶されるデータは現金の残高額である。よって、ユーザが購入した物の代金を前記ＩＣカード１０１を用いて支払うときには、携帯型記憶装置１でＩＣカード１０１に記憶される金額を読み出して、コンピュータ装置１００に送信する。コンピュータ装置１００は、送信された残高額から前記購入物の代金分を減算し、この減算した金額のデータを携帯型記憶装置１に送信する。携帯型記憶装置１は、前記送信された金額をＩＣカード１０１のＩＣ１０２に書き込む。

【００９３】このように、ユーザは、所有するＩＣカード１０１を、不特定多数のユーザが使用するコンピュータ装置１００に直接に装着せずに、自分が所有する携帯型記憶装置１にＩＣカード１０１を装着して、このＩＣカード１０１を利用することができる。また、ＩＣカード１０１のデータをコンピュータ装置１００に送信するときに、ＩＣカード１０１のデータをＫＰＳを用いた暗号化方法で暗号化するので、この暗号化されたデータが盗まれた場合にも、このデータを他人に盗用されることを防止できる。

【００９４】次に、携帯型記憶装置１に記憶するデータ等を他の電子機器に送信し、そのデータを前記他の電子機器内で処理し、その処理されたデータ等を受信して記憶するデータ処理、いわゆる依頼計算処理について説明する。

【００９５】例えば、図５に示すように、携帯型記憶装置１では、計算処理用のデータ及び計算処理プログラムを暗号化し、この暗号化されたデータ及び計算処理プログラムを計算情報としてＰＣ３０６に送信する。ＰＣ３０６では、暗号化されたデータ及び計算処理プログラムを受信して復号化する。そして、復号化された元の計算処理プログラムを用いて、復号化した元のデータを計算処理する。この後、計算処理されたデータ及び計算処理プログラムを暗号化して、計算実行結果として携帯型記憶装置１に送信する。携帯型記憶装置１では、この計算実行結果を受信して、復号化する。これにより、計算処理されたデータ及び計算処理プログラムを復元し、このデータ及び計算処理プログラムを記憶する。

【００９６】このように、携帯型記憶装置１は、データ等を他の電子機器に送信して、その他の電子機器の処理能力を借りてデータ処理を行う。このとき、前記他の電子機器が高速な処理能力を備えたコンピュータ装置であるならば、携帯型記憶装置１を所有するだけで、より迅速なデータ処理を行うことができる。

【００９７】また、携帯型記憶装置１と他の電子機器の間のデータの送受信時には、ＫＰＳを用いた暗号化方法によりデータを暗号化して送受信する。このＫＰＳによる暗号化データを盗んでも、復号鍵を持たなければ、暗号化データを復号化することは困難であるので、送受信時のデータの安全性を高めることができる。

【００９８】尚、計算処理プログラム以外のアプリケーションプログラムを用いて、計算処理以外のデータ処理を行うことも可能である。

【００９９】また、ＰＣ３０６内に所望の計算処理プログラム等のアプリケーションプログラムが記憶されてい

ることが、予め判明しているならば、このアプリケーションプログラムを送信する必要はない。

【０１００】上述したデータ処理を行うには、例えば、携帯型記憶装置１の記憶部１２を、ＰＣ３０６に接続されたハードディスクドライブ装置とみなし、この記憶部１２に記憶されるデータを処理する。

【０１０１】このときの信号の送受信の手順を、図６のフローチャートを用いて説明する。

【０１０２】まず、ステップＳ４２で、携帯型記憶装置１は、ＰＣ３０６から送信されるデータの受信可能な状態である、いわゆるスタンバイ状態となっているものとする。

【０１０３】一方、ステップＳ６２で、ＰＣ３０６は、任意の携帯型記憶装置をＰＣ３０６に接続される記憶装置、即ちハードディスクドライブ装置のうちの１つとみなすことができる状態となっている。

【０１０４】これにより、ステップＳ６４で、ＰＣ３０６のディスプレイ部には、接続可能な携帯型記憶装置の一覧表、いわゆるリストが表示される。尚、この場合には、携帯型記憶装置は１つであるので、前記リストには前記携帯型記憶装置１しか表示されない。よって、ユーザは前記携帯型記憶装置１を選択する。この選択により、ＰＣ３０６から携帯型記憶装置１に対して、ＰＣ３０６のハードディスクドライブ装置として選択したことを示す命令が送信される。

【０１０５】携帯型記憶装置１は、ステップＳ４４で、ＰＣ３０６から送信された選択命令を受信する。そして、携帯型記憶装置１は、ＰＣ３０６からドライブ装置として選択されたことを、表示部１６に表示する。

【０１０６】ユーザは、携帯型記憶装置１をＰＣ３０６のハードディスクドライブ装置のうちの１つに設定するか否かを決定する。この決定情報は、ＰＣ３０６に送信される。

【０１０７】このように、携帯型記憶装置１側で、ＰＣ３０６のハードディスクドライブ装置のうちの１つとなることを設定するか否かを決定する。従って、ＰＣ３０６の選択のみによって携帯型記憶装置１をハードディスクドライブ装置と設定し、携帯型記憶装置１に記憶されるデータを強制的に受信すること、即ち携帯型記憶装置１のデータを盗むことを防止できる。

【０１０８】この後、ステップＳ４６で、携帯型記憶装置１は、ＰＣ３０６に対して、ＩＤの送信要求命令を送信する。

【０１０９】ＰＣ３０６は、ステップＳ６６で、前記ＩＤの送信要求命令を受信し、このＩＤの送信要求命令に応じて、固有のＩＤを携帯型記憶装置１に送信する。

【０１１０】携帯型記憶装置１は、ＰＣ３０６から送信されるＰＣ３０６の固有のＩＤを受信して記憶する。また、携帯型記憶装置１は、自機の固有のＩＤをＰＣ３０６に送信する。よって、ＰＣ３０６は、携帯型記憶装置１の固有のＩＤを受信して記憶する。

【０１１１】この後、ステップＳ４８で、携帯型記憶装置１は、ＰＣ３０６の固有のＩＤ及び自機の固有の秘密プログラムを用いて暗号鍵を生成する。

【０１１２】また、ステップＳ６８で、ＰＣ３０６は、携帯型記憶装置１の固有のＩＤ及び自機の固有の秘密アルゴリズムを用いて暗号鍵を生成する。

【０１１３】次に、ステップＳ５０で、携帯型記憶装置１は、生成した暗号鍵を用いた暗号鍵プログラムにより、任意のファイルのデータを暗号化する。そして、この暗号化したデータを、暗号化信号としてＰＣ３０６に送信する。

【０１１４】ＰＣ３０６では、ステップＳ７０で、送信された暗号化信号を受信して、復号化する。この復号化により復元されたデータは、ユーザによるアプリケーションソフトウェア上の作業により、処理される。

【０１１５】そして、ＰＣ３０６は、ステップＳ７２で、前記生成した暗号鍵を用いた暗号鍵プログラムにより、前記処理データを暗号化する。ＰＣ３０６は、この暗号化されたデータを携帯型記憶装置１に送信する。

【０１１６】携帯型記憶装置１は、ステップＳ５２で、送信された暗号化信データを受信して、復号化する。これにより、復元された処理データは、記憶部１２に記憶される。

【０１１７】この後、ステップＳ５４で、携帯型記憶装置１では、ＰＣ３０６のハードディスクドライブ装置となることが解除されて、ＰＣ３０６との接続が切断される。

【０１１８】一方、ＰＣ３０６でも、ステップＳ７４で、携帯型記憶装置１をハードディスクドライブ装置のうちの１つとして設定することが解除されて、携帯型記憶装置１との接続が切断される。

【０１１９】さらに、上述した携帯型記憶装置の構成を、携帯型電話装置に備えることもできる。これにより、ユーザは、携帯型電話装置のみを携帯することで、電話通信の他に、データの送受信や処理等を行うことができる。

【０１２０】

【図面の簡単な説明】

【図１】本発明に係る携帯型通信装置を含む携帯型記憶装置の第１の実施の形態及びプリンタ装置の概略的な構成図である。

【図２】携帯型記憶装置と他の電子機器との信号の送受信を説明するための図である。

【図３】携帯型記憶装置とプリンタ装置との信号の送受信の手順を示すフローチャートである。

【図４】携帯型記憶装置の第２の実施の形態及びその具体的な実施例について説明するための図である。

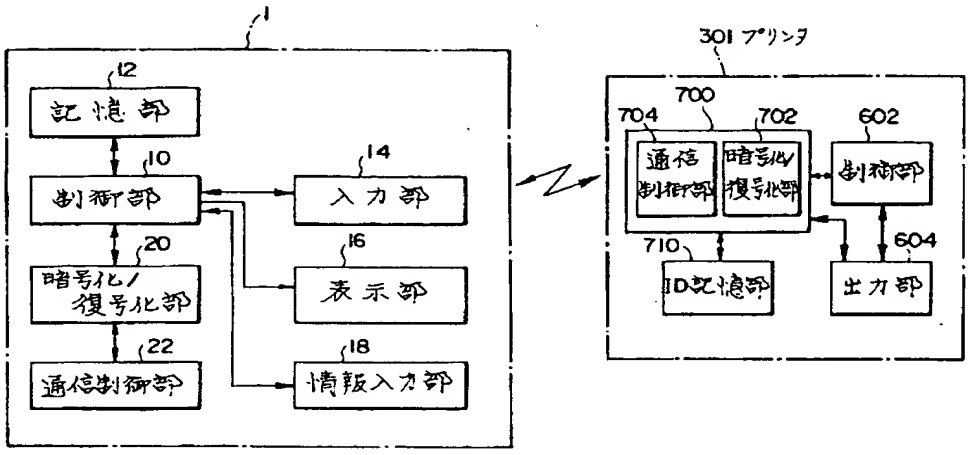
【図５】携帯型記憶装置の他の実施例について説明するための図である。

【図６】携帯型記憶装置とＰＣとの信号の送受信の手順を示すフローチャートである。

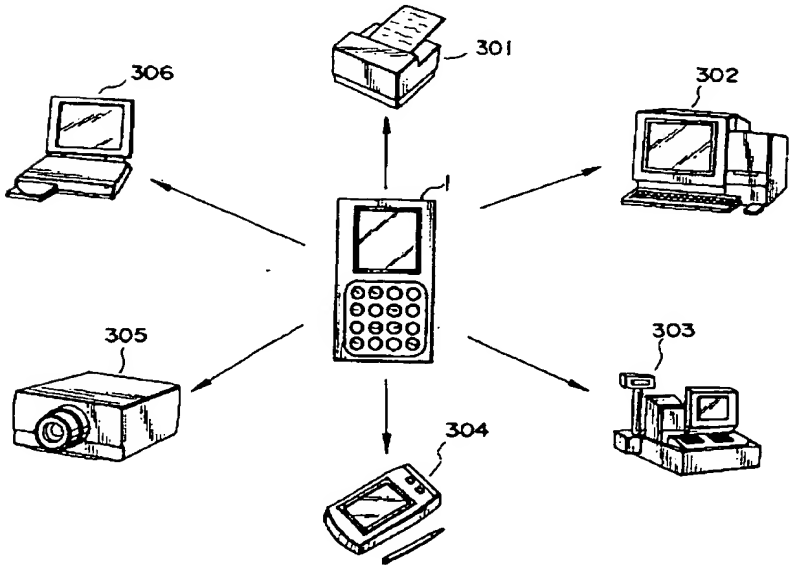
【符号の説明】

１　携帯型記憶装置
１０　制御部
１２　記憶部
１４　入力部
１６　表示部
１８　情報入力部
２０　暗号化／復号化部
２２　通信制御部

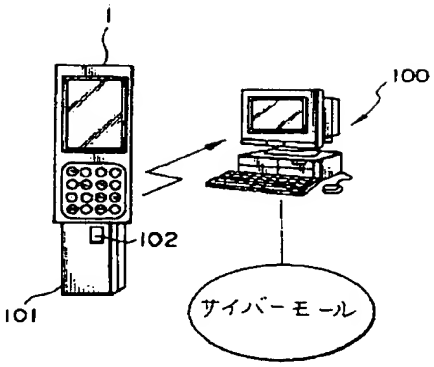
【図１】



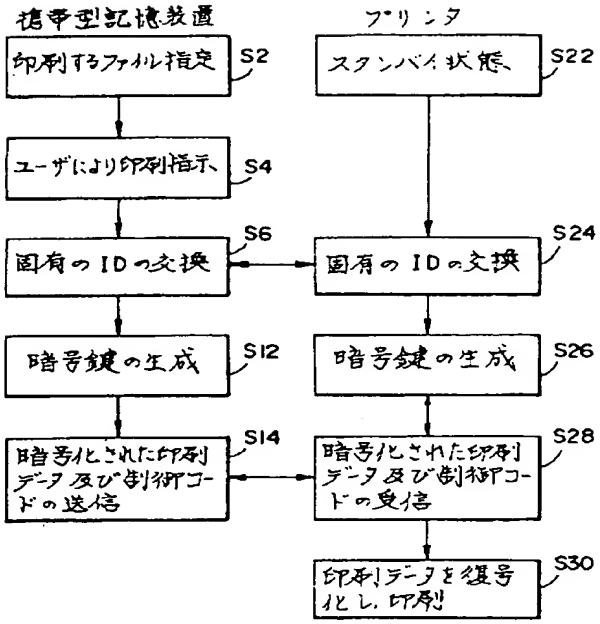
【図２】



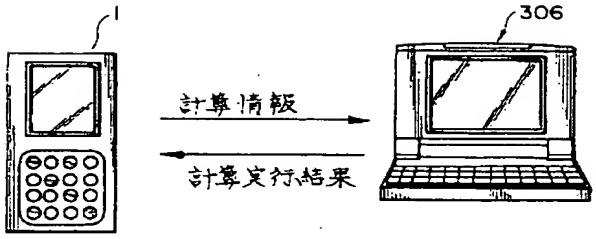
【図４】



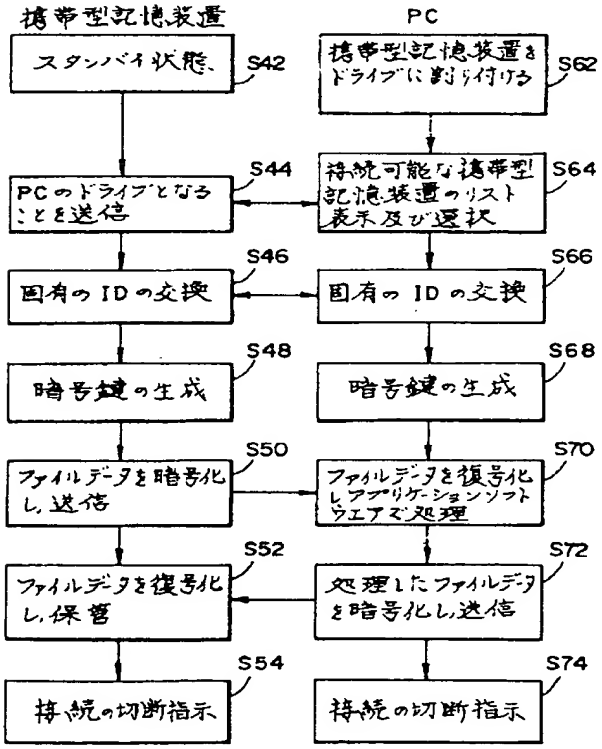
【図３】


携帯型記憶装置
プリンタ
印刷するファイル指定
S2
スタンバイ状態
S22
ユーザにより印刷指示
S4
固有のIDの交換
S6
固有のIDの交換
S24
暗号鍵の生成
S12
暗号鍵の生成
S26
暗号化された印刷データ及び制御コードの送信
S14
暗号化された印刷データ及び制御コードの受信
S28
印刷データを復号化し、印刷
S30

【図５】


1
306
計算情報
計算実行結果

【図６】


携帯型記憶装置
PC
スタンバイ状態
S42
携帯型記憶装置をドライブに割り付ける
S62
PCのドライブとなることを送信
S44
接続可能な携帯型記憶装置のリスト表示及び選択
S64
固有のIDの交換
S46
固有のIDの交換
S66
暗号鍵の生成
S48
暗号鍵の生成
S68
ファイルデータを暗号化し、送信
S50
ファイルデータを復号化しアプリケーションソフトウエアで処理
S70
ファイルデータを復号化し、保管
S52
処理したファイルデータを暗号化し送信
S72
接続の切断指示
S54
接続の切断指示
S74

フロントページの続き

(51) Int.Cl.[6]	識別記号	庁内整理番号	FI		技術表示箇所
// Ｇ０６Ｆ　12/14	３２０		Ｈ０４Ｌ　9/00	６０１Ｄ	